Notice of Allowability	Application No.	Applicant(s)	
	09/672,602	ELLISON ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Appeal Brief filed on 11/30/2005*.

2. ☒ The allowed claim(s) is/are *2-20,22-40,42-60 and 62-80*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *1/31/2006* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Thinh Nguyen (Registration No. 42,034) on January 31, 2006.

The application has been amended as follows:

3. Claims 1, 21, 41, and 61 are cancelled by virtue of this Examiner's Amendment.

4. Claims 2,22,42, and 62 are re-written in an independent form as given below.

Claim 2 (Currently Amended):

An apparatus comprising:

a digest memory to store an isolated digest in a secure environment for an isolated execution mode, the secure environment being associated with an isolated memory area accessible by at least one processor, the at least one processor operating in one of a normal execution mode and the isolated execution mode; and

an attestation key memory (AKM) device coupled to the digest memory to attest the isolated execution mode and prove validity of a program loaded into the isolated memory area using the isolated digest;

wherein the isolated digest includes at least a digest of one of a processor nub loader, a processor nub, an operating system nub, and a supervisory module loaded in an isolated execution space.

Claim 22 (Currently Amended):

A method comprising:

storing an isolated digest in a digest memory in a secure environment for an isolated execution mode, the secure environment being associated with an isolated memory area accessible by at least one processor, the at least one processor operating in one of a normal execution mode and the isolated execution mode; and

attesting the isolated execution mode and proving validity of a program loaded into the isolated memory area using an attestation key memory (AKM) device and the isolated digest;

wherein the isolated digest includes at least a digest of one of a processor nub loader, a processor nub, an operating system nub, and a supervisory module loaded in an isolated execution space.

Claim 42 (Currently Amended):

A computer program product comprising:

a machine readable medium having program code embedded therein, the computer program product comprising:

computer readable program code to store an isolated digest in a digest memory in a secure environment for an isolated execution mode, the secure environment being associated with an isolated memory area accessible by at least one processor, the at least one processor operating in one of a normal execution mode and the isolated execution mode; and

computer readable program code to attest the isolated execution mode and proving validity of a program loaded into the isolated memory area using an attestation key memory (AKM) device and the isolated digest;

wherein the isolated digest includes at least a digest of one of a processor nub loader, a processor nub, an operating system nub, and a supervisory module loaded in an isolated execution space.

Claim 62 (Currently Amended):

A system comprising:

an attestation key memory (AKM) device;

at least one processor operating in a secure environment, the at least one processor having one of a normal execution mode and an isolated execution mode;

a memory coupled to the at least one processor, the memory having an isolated memory area accessible to the at least one processor in the isolated execution mode; and

a chipset coupled to the at least one processor and the memory, the chipset having a circuit, the circuit comprising:

a digest memory to store an isolated digest used with the device to attest the isolated execution mode and prove validity of a program loaded into the isolated memory area;

wherein the isolated digest includes at least a digest of one of a processor nub loader, a processor nub, an operating system nub, and a supervisory module loaded in an isolated execution space.

Allowable Subject Matter

5. Claims 2-20, 22-40, 42-60, and 62-80 are allowed.

The following is an examiner's statement of reasons for allowance:

The above mentioned claims 2-20, 22-40, 42-60, and 62-80 are allowable because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claims 2,22,42,and 62, and subsequent dependent claims.

The CPA, in particular, does not teach nor suggest a system, method, or an apparatus comprising a digest memory to store an isolated digest used to attest the validity of a program and attest the isolated execution mode for a processor operating in

an isolated execution mode, wherein the isolated digest is a digest of one of a processor nub loader, a processor nub, an operating system nub, and a supervisory module loaded in an isolated execution space.

The present invention addresses the following drawbacks of prior art security mechanisms:

1) the lack of continued protection for modern microprocessors against attacks such as viruses, intrusions, and tampering without imposing limitations on speed performance, memory capacity and flexibility, and without the need to redesign the operating systems.

Thus this invention provides remote attestation by an attestation key memory (AKM) device to attest an isolated execution mode and to prove validity of a program loaded into an isolated memory area using an isolated digest stored in a digest memory.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
01/31/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100